

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NORTH DAKOTA
EASTERN DIVISION**

AMANDA KOFFLER, individually, and on
behalf of all others similarly situated,

Plaintiff,

v.

BRADY MARTZ & ASSOCIATES, P.C.,

Defendant.

Case No. _____

CLASS REPRESENTATION

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Amanda Koffler (“Plaintiff”), individually, and on behalf of all others similarly situated, brings this action against the Brady Martz & Associates (“Brady Martz” or “Defendant”). Plaintiff brings this action by and through her attorneys, and alleges, based upon personal knowledge as to her own actions, and based upon information and belief and reasonable investigation by her counsel as to all other matters, as follow:

I. INTRODUCTION

1. Defendant Brady Martz is an accounting, tax, and audit services firm operating based in Grand Forks, North Dakota, and operating throughout North Dakota and in northwestern Minnesota.

2. As part of its accounting operations, Defendant collects, maintains, and stores highly sensitive personal information, including, but not limited to: Social Security numbers, dates of birth, full names, addresses, telephone numbers, driver’s license numbers (collectively, “personally identifying information” or “PII”). The firm also collected medical information from its clients, including but not limited to: treatment information, diagnoses, and prescription information, medical record numbers, health insurance information, and other protected health

information (collectively, “private health information” or “PHI”). Further, Defendant also collects financial account/payment card information (“financial account information”) (collectively, with PII and PHI, “Private Information”).

3. On November 19, 2022, Defendant noticed unusual activity on its networks. It then retained independent cybersecurity specialists to investigate. On August 31, 2023, Defendant’s investigations determined that unauthorized cybercriminals accessed its information systems and databases and stole Private Information belonging to Plaintiff and Class members. On September 8, 2023, Defendant dispatched a data breach notice to individuals whose information was accessed in this incident.¹

4. As Defendant stored and handled such highly-sensitive PII, PHI, and financial account information, it had a duty and obligation to safeguard this information and prevent unauthorized third parties from accessing this data.

5. Ultimately, Defendant failed to fulfill these obligations as unauthorized cybercriminals breached Defendant’s information systems and databases and stole vast quantities of Private Information belonging to Plaintiff and Class members. This breach and the successful exfiltration of Private Information were direct, proximate, and foreseeable results of multiple failings on the part of Defendant.

6. The data breach occurred because Defendant inexcusably failed to implement reasonable security protections to safeguard its information systems and databases. Thereafter, Defendant inexcusably failed to timely detect this data breach. Prior the breach occurred, Defendant failed to inform the public that its data security practices were deficient and inadequate.

¹ This Notice and information packet that Defendant dispatched to the Maine Attorney General, which contains further information regarding the data security breach incident, is attached as **Exhibit A**.

Had Plaintiff and the Class been made aware of this fact, they would have never provided such information to Defendant.

7. In addition to the failures that caused the breach, Defendant's subsequent handling of the breach was also suspect. First, Defendant's investigation was of excessive duration, lasting a total of 285 days. Second, Defendant did not inform Plaintiff and Class members that their information was stolen until 293 days after it first discovered the intrusion. In effect, Defendant failed provide Plaintiff and Class members with even the opportunity to mitigate their damages until at least *293 days*—nearly a year—after discovering the data breach.

8. Lastly, Defendant's meager attempt to ameliorate the effects of this data breach with a brief period of complimentary credit monitoring is woefully inadequate. Much of the Private Information stolen is immutable and a limited duration of credit monitoring is nothing in the face of a life-long heightened risk of identity theft.

9. As a result of Defendant's negligent, reckless, intentional, and/or unconscionable failure to adequately satisfy its contractual, statutory, and common-law obligations, Plaintiff and Class members suffered injuries as a result of Defendant's conduct including, but not limited to:

- Lost or diminished value of their Private Information;
- Out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information;
- Lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges;
- Time needed to change usernames and passwords on their accounts;
- Time needed to investigate, correct and resolve unauthorized access to their accounts; time needed to deal with spam messages and e-mails received subsequent to the Data Breach;

- Charges and fees associated with fraudulent charges on their accounts; and the continued and increased risk of compromise to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect their Private Information.

10. Accordingly, Plaintiff brings this action on behalf of all those similarly situated to seek relief for the consequences of Defendant's failure to reasonably safeguard Plaintiff's and Class members' Private Information; its failure to reasonably provide timely notification that Plaintiff's and Class members' Private Information had been compromised by an unauthorized third party; and for intentionally and unconscionably deceiving Plaintiff and Class members concerning the status, safety, location, access, and protection of their Private Information.

II. PARTIES

Plaintiff Amanda Koffler

11. Plaintiff Amanda Koffler is a resident and citizen of Dickinson, North Dakota. Plaintiff Koffler was not aware that Defendant Brady Martz possessed her Private Information. Nonetheless, on September 12, 2023, Plaintiff Koffler received Defendant's Data Breach Notice which explained that information such as her name, date of birth, driver's license or state ID number, health information, medical information, and Social Security number were exposed in the data breach.

Defendant Brady Martz & Associates.

12. Defendant Brady Martz & Associates, P.C. is a North Dakota corporation with its principal place of business located at 401 Demers AVE, Suite 300, Grand Forks, North Dakota 58208. Defendant is an accounting, auditing, and tax services firm that employs 270 accountants along with numerous other support staff and serves over 20,000 clients.²

² <https://www.bradymartz.com/about/> (last accessed September 15, 2023).

III. JURISDICTION AND VENUE

13. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act of 2005 (“CAFA”), 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in controversy exceeds the sum of \$5,000,000, the number of class members exceeds 100, and at least one Class member is a citizen of a state different from Defendant. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

14. This Court has personal jurisdiction over Defendant because Defendant is headquartered in North Dakota.

15. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to Plaintiff’s and Class members’ claims occurred in this District.

IV. FACTUAL ALLEGATIONS

A. Defendant Brady Martz – Background

16. Defendant Brady Martz is an accounting, auditing, and tax services firm based out of Grand Forks, North Dakota. It serves 20,000 clients with a roster of 270 accountants and their supporting staff. As part of its business operations, Brady Martz collects, maintains, and stores the highly sensitive PII, PHI and financial account information provided by its clients. Upon information and belief, Brady Martz acquired this information directly from individuals or through their business/institutional clients.

17. On information and belief, Defendant had failed to implement necessary data security safeguards at the time of the Data Breach. This failure resulted in cybercriminals accessing Plaintiff’s and Class members’ Private Information.

18. Plaintiff and Class members, made their Private Information available to Defendant or Defendant's clients with the reasonable expectation that any entity with access to this information would keep that sensitive and personal information confidential and secure from illegal and unauthorized access. And, in the event of any unauthorized access, that these entities would provide them with prompt and accurate notice.

19. This expectation was objectively reasonable and based on an obligation imposed on Defendant by statute, regulations, industrial custom, and standards of general due care.

20. Unfortunately for Plaintiff and Class members, Defendant failed to carry out its duty to safeguard sensitive Private Information and provide adequate data security. As a result, it failed to protect Plaintiff and Class members from having their Private Information accessed and stolen during the Data Breach.

B. The Data Breach

21. Upon information and belief, cybercriminals breached Defendant's information systems and databases some time before November 19, 2023, the date that Defendant purportedly first discovered "unusual activity" on its systems.³

22. Defendant then launched an investigation with the assistance of third-party data security specialists. This investigation, which purportedly concluded on August 31, 2023, determined that cybercriminals had successfully breached the Defendant's systems some time prior to November 19, 2023, and had accessed and stolen Plaintiff's and Class members' Private Information.⁴

³ Ex. A.

⁴ Ex. A.

23. On September 8, 2023, Defendant issued notice to all individuals believed to have been impacted by the data security incident.⁵

24. Defendant estimates that the Private Information belonging to at least 53,524 individuals was compromised in this incident.⁶

C. Defendant's Many Failures Both Prior to and Following the Breach

25. Defendant collects and maintains vast quantities of Private Information belonging to Plaintiff and Class members as part of its normal operations. The data breach occurred as direct, proximate, and foreseeable results of multiple failings on the part of Defendant.

26. First, Defendant inexcusably failed to implement reasonable security protections to safeguard its information systems and databases.

27. Second, Defendant inexcusably failed to timely detect this data breach, with Defendant's IT agents only becoming aware of the intrusion on November 19, 2022. Upon information and belief, the data breach began prior to November 19, 2020, and the cybercriminals had ample time to access, evaluate, and steal the sensitive Private Information belonging to Defendant's clients, including Private Information concerning Plaintiff and Class members.

28. Third, Defendant failed to inform the public that its data security practices were deficient and inadequate. Had Plaintiff and the Class members been aware that Defendant did not have adequate safeguards in place to protect such sensitive Private Information, they would have never provided such information to Defendant, and Defendant's institutional clients would have refused to engage Defendant's services and provide their customers' highly sensitive Personal Information.

⁵ Ex. A.

⁶ <https://apps.web.maine.gov/online/aevviewer/ME/40/9b9f089f-c004-4fa5-a3a7-ad33820bbcd1.shtml> (last accessed September 15, 2023)

29. In addition to the failures that lead to the successful breach, Defendant's failings in handling the breach and responding to the incident exacerbated the resulting harm to Plaintiff and the Class.

30. First, Defendant's investigation of excessive duration, lasting a total of 285 days from the date when the breach was discovered to the date that when it was discovered that sensitive information had been compromised.

31. Second, Defendant did not inform Plaintiff and Class members that their information was stolen during the entirety of this 285-day investigation. Defendant did not notify Plaintiff and Class members that their Private Information was compromised until 293 days—*nearly 1 year*—after Defendant first discovered the breach. This delay in informing the Class virtually ensured that the cybercriminals who stole this Private Information could monetize, misuse and/or disseminate that Private Information before Plaintiff and Class members could take affirmative steps to protect their sensitive information. As a result, Plaintiff and Class members will suffer indefinitely from the substantial and concrete risk that their identities will be (or already have been) stolen and misappropriated.

32. Third, Defendant's attempt to ameliorate the effects of this data breach with a limited period of complimentary credit monitoring is woefully inadequate. Plaintiff's and Class members' Private Information was accessed and acquired by cybercriminals for the express purpose of misusing the data. As a consequence, they face the real, immediate, and likely danger of identity theft and misuse of their Private Information. Identity theft can, and in some circumstances already has, caused irreparable harm to their personal, financial, reputational, and future well-being. This harm is even more acute because much of the stolen Private Information, such as healthcare data and Social Security numbers, is immutable.

33. In short, Defendant's myriad failures, including the failure to timely detect an intrusion and failure to timely notify Plaintiff and Class members that their personal and medical information had been stolen due to Defendant's security failures, allowed unauthorized individuals to access, misappropriate, and misuse Plaintiff's and Class members' Private Information for nearly a year before Defendant finally granted victims the opportunity to take proactive steps to defend themselves and mitigate the near- and long-term consequences of the Data Breach.

D. Data Breaches Pose Significant Threats

34. Data breaches have become a constant threat that, without adequate safeguards, can expose personal data to malicious actors. It is well known that PII, Social Security numbers in particular, is an invaluable commodity and a frequent target of hackers.

35. In 2022, the Identity Theft Resource Center's Annual End-of-Year Data Breach Report listed 1,802 total compromises involving 422,143,312 victims for 2022, which was just 50 compromises short of the current record set in 2021.⁷ The HIPAA Journal's 2022 Healthcare Data Breach Report reported 707 compromises involving healthcare data, which is just 8 shy of the record of 715 set in 2021 and still double that of the number of similar such compromises in 2017 and triple the number of compromises in 2012.⁸

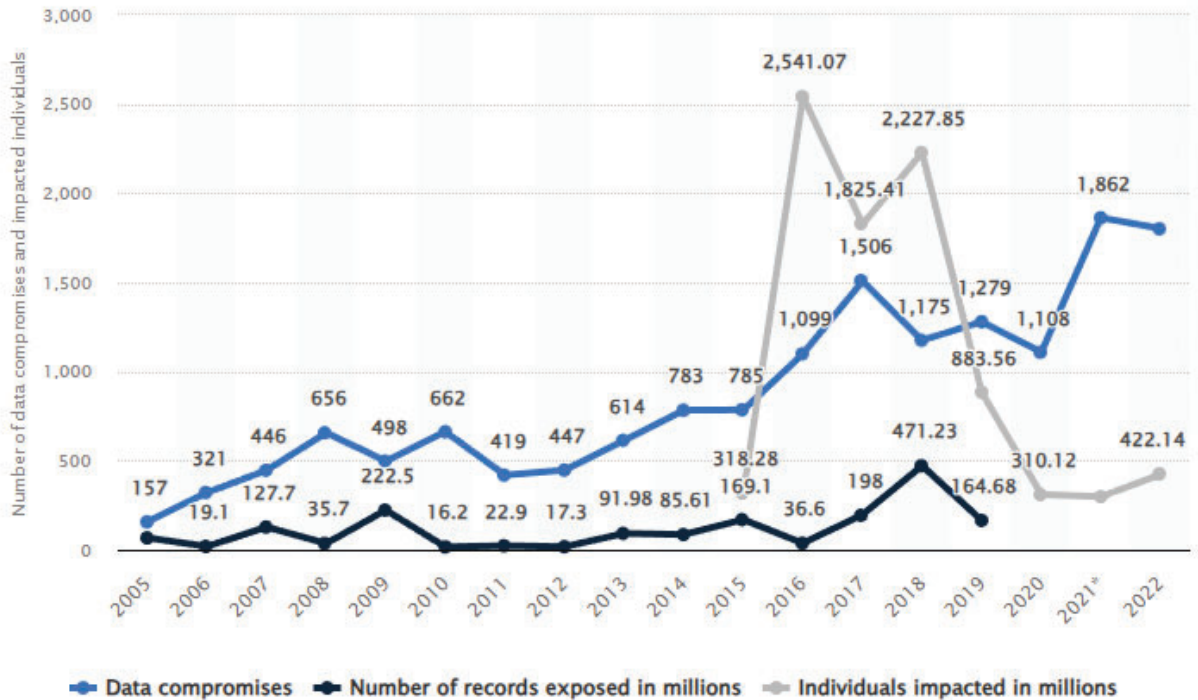
36. Statista, a German entity that collects and markets data relating to, among other things, data breach incidents and the consequences thereof, confirms that the number of data breaches has been steadily increasing since it began a survey of data compromises in 2005 with 157 compromises reported that year, to a peak of 1,862 in 2021, to 2022's total of 1,802.⁹ The

⁷ *2022 End of Year Data Breach Report*, Identity Theft Resource Center (January 25, 2023), available at: https://www.idtheftcenter.org/publication/2022-data-breach-report/?utm_source=press+release&utm_medium=web&utm_campaign=2022+Data+Breach+Report+.

⁸ *2022 Healthcare Data Breach Report*, The HIPAA Journal (January 24, 2023), available at: <https://www.hipaajournal.com/2022-healthcare-data-breach-report/>.

⁹ *Annual Number of Data Breaches and Exposed Records in the United States from 2005*

number of impacted individuals has also risen precipitously from approximately 318 million in 2015 to 422 million in 2022, which is an increase of nearly 50%.¹⁰



37. This stolen PII is then routinely traded on dark web black markets as a simple commodity, with Social Security numbers being sold for as little as \$2.99, and passports retailing for as little as \$15.¹¹

38. In addition, the severity of the consequences of a compromised Social Security number belies the ubiquity of stolen numbers on the dark web. Criminals and other unsavory elements can fraudulently take out loans under the victims' name, open new lines of credit, and cause other serious financial difficulties for victims:

to 2022, Statista, available at: <https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/> (last accessed last accessed September 15, 2023).

¹⁰ *Id.*

¹¹ *What is your identity worth on the dark web?* Cybernews (September 28, 2021), available at: <https://cybernews.com/security/whats-your-identity-worth-on-dark-web/>.

[a] dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.¹²

This is exacerbated by the fact that the problems arising from a compromised Social Security number are exceedingly difficult to resolve. A victim is forbidden from proactively changing his or her number unless and until it is actually misused and harm has already occurred. And even this delayed remedial action is unlikely to undo the damage already done to the victims:

Keep in mind that a new number probably won't solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.¹³

39. The most sought after and expensive information on the dark web are stolen medical records, which command prices from \$250 to \$1,000 each.¹⁴ Medical records are considered the most valuable because unlike credit cards, which can easily be canceled, and Social Security numbers, which can be changed, medical records contain “a treasure trove of unalterable data points, such as a patient's medical and behavioral health history and demographics, as well as their health insurance and contact information.”¹⁵ With this bounty of ill-gotten information,

¹² United States Social Security Administration, *Identity Theft and Your Social Security Number*, United States Social Security Administration (July 2021), available at: <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last accessed September 15, 2023).

¹³ *Id.*

¹⁴ Paul Nadrag, Capsule Technologies, *Industry Voices—Forget credit card numbers. Medical records are the hottest items on the dark web*, Fierce Healthcare (January 26, 2021), available at: <https://www.fiercehealthcare.com/hospitals/industry-voices-forget-credit-card-numbers-medical-records-are-hottest-items-dark-web>.

¹⁵ *Id.*

cybercriminals can steal victims' public and insurance benefits and bill medical charges to victims' accounts.¹⁶ Cybercriminals can also change the victims' medical records, which can lead to misdiagnosis or mistreatment when the victims seek medical treatment.¹⁷ Victims of medical identity theft could even face prosecution for drug offenses when cybercriminals use their stolen information to purchase prescriptions for sale in the drug trade.¹⁸

40. The wrongful use of compromised medical information is known as medical identity theft and the damage resulting from medical identity theft is routinely far more serious than the harm resulting from the theft of simple PII. Victims of medical identity theft spend an average of \$13,500 to resolve problems arising from medical identity theft and there are currently no laws limiting a consumer's liability for fraudulent medical debt (in contrast, a consumer's liability for fraudulent credit card charges is capped at \$50).¹⁹ It is also "considerably harder" to reverse the damage from the aforementioned consequences of medical identity theft.²⁰

41. Instances of Medical identity theft have grown exponentially over the years from approximately 6,800 cases in 2017 to just shy of 43,000 in 2021, which represents a seven-fold increase in the crime.²¹

42. Additionally, with just a minimal amount of a person's data, identity thieves can take over the victim's identity—or attempt other forms of hacking crimes against the individual to obtain more data for additional forms of identity theft.

¹⁶ *Medical Identity Theft in the New Age of Virtual Healthcare*, IDX (March 15, 2021), available at <https://www.idx.us/knowledge-center/medical-identity-theft-in-the-new-age-of-virtual-healthcare>. See also Michelle Andrews, *The Rise of Medical Identity Theft*, Consumer Reports (August 25, 2016), available at <https://www.consumerreports.org/health/medical-identity-theft-a1699327549/>.

¹⁷ *Id.*

¹⁸ *Id.*

¹⁹ Medical Identity Theft, AARP (March 25, 2022), available at: <https://www.aarp.org/money/scams-fraud/info-2019/medical-identity-theft.html>.

²⁰ *Id.*

²¹ *Id.*

43. For example, with just an individual's name and date of birth, a cybercriminal perform "social engineering" to obtain even more of the victim's Private Information. Social engineering consists of the criminal using previously acquired information to manipulate and trick the victim into disclosing more confidential or personal information, and includes means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victim.

44. Criminals then piecing together the different bits and pieces of compromised Personal Information to development of "Fullz" packages.²² To create a "Fullz" package, hackers compile multiple sources of Private Information and marry the information to unregulated data available elsewhere to assemble complete profiles of the individuals.

45. In light of the dozens of high-profile health and medical information data breaches that have been reported in recent years, entities like Defendant charged with maintaining and securing PII and PHI should know the importance of protecting that information from unauthorized disclosure. Indeed, Defendant knew, or certainly should have known, of the recent and high-profile

²² "Fullz" is a term used to connote data that provide the full panoply of Private Information information of the victim, including but not limited to, the name, address, credit card information, Social Security number, date of birth, and more. Fullz are sold at much higher prices than simple personal information, such as credit card credentials, commanding up to \$100 per record (or more) on the dark web. Fullz packages can be used in various ways for identity and financial theft, including performing bank transactions over the phone with the authentication details in the Fullz package. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.,* Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), <https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-1/>(<https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn>).

data breaches in the health care industry: UnityPoint Health, Lifetime Healthcare, Inc., Community Health Systems, Kalispell Regional Healthcare, Anthem, Premera Blue Cross, and many others.²³

46. In addition, the Federal Trade Commission (“FTC”) has brought dozens of cases against companies that have engaged in unfair or deceptive practices involving inadequate protection of consumers’ personal data, including recent cases concerning health-related information against LabMD, Inc., SkyMed International, Inc., and others. The FTC publicized these enforcement actions to place companies like Defendant on notice of their obligation to safeguard Private Information.²⁴

47. Given the nature of Defendant’s Data Breach, as well as the length of the time Defendant’s networks were breached and the long delay in notification to the Class, it is foreseeable that the compromised Private Information has been or will be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Plaintiff’s and Class members’ Private Information can easily obtain Plaintiff’s and Class members’ tax returns or open fraudulent credit card accounts in Class members’ names.

48. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because credit card victims can cancel or close credit and debit card accounts.²⁵ The

²³ See e.g., *Healthcare Data Breach Statistics*, HIPAA Journal, available at: <https://www.hipaajournal.com/healthcare-data-breach-statistics> (last accessed September 15, 2023).

²⁴ See e.g., *In the Matter of SKYMED INTERNATIONAL, INC.*, C-4732, 1923140 (F.T.C. Jan. 26, 2021).

²⁵ See Jesse Damiani, *Your Social Security Number Costs \$4 On The Dark Web, New Report Finds*, *Forbes* (Mar 25, 2020), available at <https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1>. See also *Why Your Social Security Number Isn’t as Valuable as Your Login Credentials*, Identity Theft Resource Center (June 18, 2021), available at <https://www.idtheftcenter.org/post/why-your-social-security-number-isnt-as-valuable-as-your-login-credentials/>.

information compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change.

49. To date, Defendant has offered its consumers limited identity theft monitoring services. The offered services are inadequate to protect Plaintiff and the Class from the threats they will face for years to come, particularly in light of the Private Information at issue here.

50. Despite the prevalence of public announcements of data breach and data security compromises, its own acknowledgment of the risks posed by data breaches, and its own acknowledgment of its duties to keep Private Information private and secure, Defendant failed to take appropriate steps to protect the Private Information of Plaintiff and the Class from misappropriation. As a result, the injuries to Plaintiff and the Class were directly and proximately caused by Defendant’s failure to implement or maintain adequate data security measures for its clients and clients’ clients.

E. Defendant Had a Duty and Obligation to Protect Private Information

51. Defendant has an obligation to protect the Private Information belonging to Plaintiff and Class members. First, this obligation was mandated by government regulations and state laws, including HIPAA and FTC rules and regulations. Second, this obligation arose from industry standards regarding the handling of sensitive PII and medical records. Plaintiff and Class members provided, and Defendant obtained, their information on the understanding that it would be protected and safeguarded from unauthorized access or disclosure.

1. *HIPAA Requirements and Violation*

52. HIPAA requires, *inter alia*, that Covered Entities and Business Associates implement and maintain policies, procedures, systems and safeguards that ensure the confidentiality and integrity of consumer and patient PII and PHI, protect against any reasonably

anticipated threats or hazards to the security or integrity of consumer and patient PII and PHI, regularly review access to data bases containing protected information, and implement procedures and systems to detect, contain, and correct any unauthorized access to protected information. *See* 45 CFR § 164.302, *et seq.*

53. HIPAA, as applied through federal regulations, also requires private information to be stored in a manner that renders it, “unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology. . .” 45 CFR § 164.402.

54. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414 require Defendant to provide notice of the Data Breach to each affected individual “without unreasonable delay and ***in no case later than 60 days following discovery of the breach***” (emphasis added).

55. Upon information and belief, Defendant failed to implement and/or maintain procedures, systems, and safeguards to protect the PII and PHI belonging to Plaintiff and the Class from unauthorized access and disclosure.

56. Upon information and belief, Defendant’s security failures include, but are not limited to:

- a. Failing to maintain an adequate data security system to prevent data loss;
- b. Failing to mitigate the risks of a data breach and loss of data;
- c. Failing to ensure the confidentiality and integrity of electronic protected health information Defendant creates, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);
- d. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);
- e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

- f. Failing to identify and respond to suspected or known security incidents;
- g. Failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii);
- h. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR 164.306(a)(2);
- i. Failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3);
- j. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce, in violation of 45 CFR 164.306(a)(94); and
- k. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq.*

57. Upon information and belief, Defendant also failed to store the information it collected in a manner that rendered it, "unusable, unreadable, or indecipherable to unauthorized persons," in violation of 45 CFR § 164.402.

58. Defendant also violated the HIPAA Breach Notification Rule since it did not inform Plaintiff and the Class members about the breach until 293 days after it first discovered the breach.

59. Because Defendant has failed to comply with HIPAA, while monetary relief may cure some of Plaintiff's and Class members' injuries, injunctive relief is also necessary to ensure Defendant's approach to information security is adequate and appropriate going forward. Defendant still maintains the PHI and other highly sensitive PII of its clients and clients' clients, including Plaintiff and Class members. Without the supervision of the Court through injunctive relief, Plaintiff's and Class members' Private Information remains at risk of subsequent data breaches.

2. *FTC Act Requirements and Violations*

60. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

61. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.²⁶ The guidelines note businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.²⁷ The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.²⁸ Defendant clearly failed to do any of the foregoing, as evidenced by the length of the Data Breach, the fact that the Breach went undetected, and the amount of data exfiltrated.

²⁶ *Protecting Personal Information: A Guide for Business*, Federal Trade Comm'n (October 2016), available at <https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business> (last accessed September 15, 2023).

²⁷ *Id.*

²⁸ *Id.*

62. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

63. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

64. Additionally, the FTC Health Breach Notification Rule obligates companies that suffered a data breach to provide notice to every individual affected by the data breach, as well as notifying the media and the FTC. *See* 16 CFR 318.1, *et seq.*

65. As evidenced by the Data Breach, Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

66. Defendant was fully aware of its obligation to protect the Private Information of its clients and clients' clients, including Plaintiff and the Class, and on information and belief, Defendant is a sophisticated company that regularly handles and stores sensitive information, including protected health information, belonging to its clients and clients' clients.

67. Defendant had and continues to have a duty to exercise reasonable care in collecting, storing, and protecting the Private Information from the foreseeable risk of a data

breach. The duty arises out of the special relationship that exists between Defendant and Plaintiff and Class members. Defendant alone had the exclusive ability to implement adequate security measures to its cyber security network to secure and protect Plaintiff's and Class members' Private Information.

3. *Industry Standards and Noncompliance*

68. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

69. Some industry best practices that should be implemented by businesses dealing with sensitive PHI like Defendant include but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendant failed to follow some or all of these industry best practices.

70. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendant failed to follow these cybersecurity best practices.

71. Defendant should have also followed the minimum standards of any one of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1,

PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

72. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

F. Plaintiff and the Class Suffered Harm Resulting from the Data Breach

73. Like any data hack, the Data Breach presents major problems for all affected.²⁹

74. The FTC warns the public to pay particular attention to how they keep personally identifying information including Social Security numbers and other sensitive data. As the FTC notes, "once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance."³⁰

75. The ramifications of Defendant's failure to properly secure Plaintiff's and Class members' Private Information are severe. Identity theft occurs when someone uses another person's financial, and personal information, such as that person's name, address, Social Security number, and other information, without permission in order to commit fraud or other crimes.

76. According to data security experts, one out of every four data breach notification recipients become a victim of identity fraud.

77. Furthermore, PII has a long shelf-life because it contains different forms of personal information, it can be used in more ways than one, and it typically takes time for an information breach to be detected.

²⁹ Paige Schaffer, *Data Breaches' Impact on Consumers*, Insurance Thought Leadership (July 29, 2021), available at <https://www.insurancethoughtleadership.com/cyber/data-breaches-impact-consumers>.

³⁰ *Warning Signs of Identity Theft*, Federal Trade Comm'n, available at <https://www.identitytheft.gov/#/Warning-Signs-of-Identity-Theft> (last accessed September 15, 2023).

78. Accordingly, Defendant's wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiff and the Class at an imminent, immediate, and continuing increased risk of identity theft and identity fraud. According to a recent study published in the scholarly journal "Preventive Medicine Reports", public and corporate data breaches correlate to an increased risk of identity theft for victimized consumers.³¹ The same study also found that identity theft is a deeply traumatic event for the victims, with more than a quarter of victims still experiencing sleep problems, anxiety, and irritation even six months after the crime.³²

79. There is also a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that has not yet been exploited by cybercriminals presents a concrete risk that the cybercriminals who now possess Class members' Private Information will do so at a later date or re-sell it.

80. Data breaches have also proven to be costly for affected organizations as well, with the average cost to resolve being \$4.45 million dollars in 2023.³³ The average cost to resolve a data breach involving health information, however, is more than double this figure at \$10.92 million.³⁴

81. The theft of medical information, beyond the theft of more traditional forms of PII, is especially harmful for victims. Medical identity theft, the misuse of stolen medical records and information, has seen a seven-fold increase over the last five years and this explosive growth far

³¹ David Burnes, Marguerite DeLiema, Lynn Langton, *Risk and protective factors of identity theft victimization in the United States*, Preventive Medicine Reports, Volume 17 (January 23, 2020), available at <https://www.sciencedirect.com/science/article/pii/S2211335520300188?via%3Dihub>.

³² *Id.*

³³ *Cost of a Data Breach Report 2023*, IBM Security, available at https://www.ibm.com/reports/data-breach?utm_content=SRCWW&p1=Search&p4=43700072379268622&p5=p&gclid=CjwKCAjwxOymBhAFEiwAnodBLGiGtWfjX0vRlNbx6p9BpWaOo9eZY1i6AMAc6t9S8IKsxdnbBVeUbxoCtk8QAvD_BwE&gclid=aw.ds (last accessed September 15, 2023).

³⁴ *Id.*

outstrips the increase in incidence of traditional identity theft.³⁵ Medical Identity Theft is especially nasty for victims because of the lack of laws that limit a victim's liabilities and damages from this type of identity theft (e.g., a victim's liability for fraudulent credit card charges is capped at \$50), the unalterable nature of medical information, the sheer costs involved in resolving the fallout from a medical identity theft (victims spend, on average, \$13,500 to resolve problems arising from this crime), and the risk of criminal prosecution under anti-drug laws.³⁶

82. In response to the Data Breach, Defendant offered to provide certain individuals whose Private Information was exposed in the Data Breach with limited credit monitoring services. However, this falls short of what is necessary to protect against the lifelong risk of harm imposed on Plaintiff and Class members by Defendant's failures.

83. Moreover, the credit monitoring offered by Defendant is fundamentally inadequate to protect them from the injuries resulting from the unauthorized access and exfiltration of their sensitive Private Information.

84. Here, due to the Breach, Plaintiff and Class members have been exposed to injuries that include, but are not limited to:

- a. Theft of Private Information;
- b. Costs associated with the detection and prevention of identity theft and unauthorized use of financial accounts as a direct and proximate result of the Private Information stolen during the Data Breach;
- c. Damages arising from the inability to use accounts that may have been compromised during the Data Breach;
- d. Costs associated with spending time to address and mitigate the actual and future consequences of the Data Breach, such as finding fraudulent charges, cancelling and reissuing payment cards, purchasing credit monitoring and identity theft protection services, placing freezes and alerts on their credit

³⁵ Medical Identity Theft, AARP (March 25, 2022), available at: <https://www.aarp.org/money/scams-fraud/info-2019/medical-identity-theft.html>.

³⁶ *Id.*

reports, contacting their financial institutions to notify them that their personal information was exposed and to dispute fraudulent charges, imposition of withdrawal and purchase limits on compromised accounts, including but not limited to lost productivity and opportunities, time taken from the enjoyment of one's life, and the inconvenience, nuisance, and annoyance of dealing with all issues resulting from the Data Breach, if they were fortunate enough to learn of the Data Breach despite Defendant's delay in disseminating notice in accordance with state law;

- e. The imminent and impending injury resulting from potential fraud and identity theft posed because their Private Information is exposed for theft and sale on the dark web; and
- f. The loss of Plaintiff's and Class members' privacy.

85. Plaintiff and Class members have suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their Private Information being accessed by cybercriminals. Specifically, the unauthorized access of Plaintiff's and Class members' Private Information, especially their Social Security numbers, puts Plaintiff and the Class at risk of identity theft indefinitely, and well beyond the limited period of credit monitoring that Defendant offered victims of the Breach.

86. As a direct and proximate result of Defendant's acts and omissions in failing to protect and secure Private Information, Plaintiff and Class members have been placed at a substantial risk of harm in the form of identity theft, and have incurred and will incur actual damages in an attempt to prevent identity theft.

87. Plaintiff retains an interest in ensuring there are no future breaches, in addition to seeking a remedy for the harms suffered as a result of the Data Breach on behalf of both herself and similarly situated individuals whose Private Information was accessed in the Data Breach.

G. Experiences Specific to Plaintiff

Plaintiff Amanda Koffler's Experience

88. Plaintiff Amanda Koffler does not know how Brady Martz acquired her Private Information. She believes that she provided this information to an entity that was a client of Brady Martz.

89. On or about September 12, 2023, Plaintiff Koffler received Defendant's data breach notice. The notice informed her that her information had been improperly accessed and obtained by third parties. This notice explained that the following information could have been compromised in the breach: name, date of birth, driver's license number, state ID number, health insurance information, medical information, and Social Security Number.

90. Plaintiff Koffler experienced a massive uptick in the number of spam calls and emails which started in December 2022 or January 2023 and continues to present day. Given the timeline of the breach, Plaintiff Koffler now believes that this dramatic uptick in spam is the result of the Data Breach.

91. After learning of the Breach, Plaintiff Koffler has made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. She has also spent several hours dealing with the Data Breach, valuable time she otherwise would have spent on other activities, including, but not limited to, work and recreation.

92. As a result of the Data Breach, Plaintiff Koffler has suffered anxiety due to the public dissemination of her personal information, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and using her private information for purposes of identity theft and fraud. Plaintiff Koffler is

concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

93. Plaintiff Koffler suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her Private Information, a form of property that Defendant obtained from her; (b) violation of her privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

94. As a result of the Data Breach, Plaintiff Koffler anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Plaintiff Koffler is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

V. CLASS REPRESENTATION ALLEGATIONS

95. Plaintiff brings this action on behalf of herself and, pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), a Class of:

All persons in the United States whose Private Information was accessed in the Data Breach.

Excluded from the Class are Defendant, its executives and officers, and the Judge(s) assigned to this case. Plaintiff reserves the right to modify, change or expand the Class definition after conducting discovery.

96. In the alternative, Plaintiff brings this action on behalf of herself and, pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), a subclass of:

All persons who are residents of the State of North Dakota whose Private Information was accessed in the Data Breach (the “North Dakota Subclass”).

Excluded from the Subclass are Defendant, its executives and officers, and the Judge(s) assigned to this case.

97. Numerosity: Upon information and belief, the Class is so numerous that joinder of all members is impracticable with the number of affected individuals estimated to be 53,524.³⁷ The exact number and identities of individual members of the Class are unknown at this time, such information being in the sole possession of Defendant and obtainable by Plaintiff only through the discovery process. The members of the Class will be identifiable through information and records in Defendant's possession, custody, and control.

98. Existence and Predominance of Common Questions of Fact and Law: Common questions of law and fact exist as to all members of the Class. These questions predominate over the questions affecting individual Class members. These common legal and factual questions include, but are not limited to:

- a. When Defendant learned of the Data Breach;
- b. Whether hackers obtained Class members' Private Information via the Data Breach;
- c. Whether Defendant's response to the Data Breach was adequate;
- d. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;
- e. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations, industry standards, and/or its own promises and representations;
- f. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;
- g. Whether Defendant owed a duty to Class members to safeguard their Private Information;

³⁷ <https://apps.web.maine.gov/online/aevviewer/ME/40/9b9f089f-c004-4fa5-a3a7-ad33820bbcd1.shtml> (last accessed September 15, 2023).

- h. Whether Defendant breached its duty to Class members to safeguard their Private Information;
- i. Whether Defendant had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and the Class members;
- j. Whether Defendant breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class members;
- k. Whether Defendant's conduct violated the FTCA, HIPAA, and/or the Consumer Protection Act invoked herein;
- l. Whether Defendant's conduct was negligent;
- m. Whether Defendant's conduct was *per se* negligent;
- n. Whether Defendant was unjustly enriched;
- o. What damages Plaintiff and Class members suffered as a result of Defendant's misconduct;
- p. Whether Plaintiff and Class members are entitled to actual and/or statutory damages;
- q. Whether Plaintiff and Class members are entitled to additional credit or identity monitoring and monetary relief; and
- r. Whether Plaintiff and Class members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

99. Typicality: All of Plaintiff's claims are typical of the claims of the Class since Plaintiff and all members of the Class had their Private Information compromised in the Data Breach. Plaintiff's claims and damages are also typical of the Class because they resulted from Defendant's uniform wrongful conduct. Likewise, the relief to which Plaintiff are entitled to is typical of the Class because Defendant has acted, and refused to act, on grounds generally applicable to the Class.

100. Adequacy: Plaintiff is an adequate class representative because her interests do not materially or irreconcilably conflict with the interests of the Class she seeks to represent, she has retained counsel competent and highly experienced in complex class action litigation, and she intends to prosecute this action vigorously. Plaintiff and her counsel will fairly and adequately protect the interests of the Class. Neither Plaintiff nor her counsel have any interests that are antagonistic to the interests of other members of the Class.

101. Superiority: Compared to all other available means of fair and efficient adjudication of the claims of Plaintiff and the Class, a class action is the most superior. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of individual prosecution of the complex and extensive litigation necessitated by Defendant's conduct. It would be virtually impossible for members of the Class individually to effectively redress the wrongs done to them. Even if the members of the Class could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties and to the court system presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Members of the Class can be readily identified and notified based on, *inter alia*, Defendant's records and databases.

VI. CAUSES OF ACTION

COUNT I **NEGLIGENCE**

(By Plaintiff on behalf of the Class, or, in the alternative, the North Dakota Subclass)

102. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

103. Defendant owes a duty of care to protect the Private Information belonging to Plaintiff and Class members. Defendant also owes several specific duties including, but not limited to, the duty:

- a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;
- b. to protect Private Information belonging to its clients and clients' clients using reasonable and adequate security procedures and systems compliant with industry standards;
- c. to have procedures in place to detect the loss or unauthorized dissemination of Private Information in its possession;
- d. to employ reasonable security measures and otherwise protect the Private Information of Plaintiff and Class members pursuant to the FTCA;
- e. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and
- f. to promptly notify Plaintiff and Class members of the Data Breach, and to precisely disclose the type(s) of information compromised.

104. Defendant also owes this duty because Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 requires Defendant to use reasonable measures to protect confidential data.

105. Defendant also owes this duty because industry standards mandate that Defendant protect any confidential private information within its possession and control.

106. Defendant also owes this duty because it had a special relationship with Plaintiff's and Class members. Plaintiff and Class members entrusted their Private Information to Defendant on the understanding that adequate security precautions would be taken to protect this information. Furthermore, only Defendant had the ability to protect its systems and the Private Information stored on them from attack.

107. Defendant also owes a duty to timely disclose any unauthorized access and/or theft of the Private Information belonging to Plaintiff and the Class. This duty exists to allow Plaintiff

and the Class the opportunity to undertake appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their Private Information.

108. Defendant breached its duties to Plaintiff and the Class by failing to take reasonable appropriate measures to secure, protect, and/or otherwise safeguard the Private Information belonging to Plaintiff and Class members.

109. Defendant also breached the duties it owed to Plaintiff and the Class by failing to timely and accurately disclose to Plaintiff and Class members that their Private Information had been improperly acquired and/or accessed.

110. As a direct and proximate result of Defendant's conduct, Plaintiff and the Class were damaged. These damages include, and are not limited to:

- Lost or diminished value of their Private Information;
- Out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information;
- Lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges;
- Permanent increased risk of identity theft.

111. Plaintiff and Class members were foreseeable victims of any inadequate security practices on the part of Defendant and the damages they suffered were the foreseeable result of the aforementioned inadequate security practices.

112. In failing to provide prompt and adequate individual notice of the Data Breach, Defendant also acted with reckless disregard for the rights of Plaintiff and Class members.

113. Plaintiff and the Class are entitled to damages in an amount to be proven at trial and injunctive relief requiring Defendant to, *inter alia*, strengthen its data security systems and

monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class members.

COUNT II
NEGLIGENCE *PER SE*

(By Plaintiff on behalf of the Class, or, in the alternative, the North Dakota Subclass)

114. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

115. Section 5 of the FTCA imposes a duty on Defendant to provide fair and adequate data security to secure, protect, and/or otherwise safeguard the Private Information of Plaintiff and Class members.

116. HIPAA imposes a duty on Defendant to implement reasonable safeguards to protect Plaintiff's and Class members' Private Information. 42 U.S.C. § 1302(d), *et seq.*

117. HIPAA also requires Defendant to render unusable, unreadable, or indecipherable all Private Information it collected. Defendant was required to do so through "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key." *See* definition of "encryption" at 45 C.F.R. § 164.304.

118. In the event of a data breach, HIPAA obligates Covered Entities and Business Associates to notify affected individuals, prominent media outlets, and the Secretary of the Department of Health and Human Services of the data breach without unreasonable delay and in no event later than 60 days after discovery of the data breach. 45 CFR § 164.400, *et seq.*

119. Defendant violated the FTCA and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to secure, protect, and/or otherwise safeguard Plaintiff's and Class members' Private Information.

120. Defendant violated HIPAA by failing to properly encrypt the Private Information it collected.

121. Defendant violated HIPAA by unduly delaying reasonable notice of the actual breach; in this case by 293 days.

122. Defendant's failure to comply with HIPAA and the FTCA constitutes negligence *per se*.

123. Plaintiff and Class members are within the class of persons that the FTCA and HIPAA are intended to protect.

124. It was reasonably foreseeable that the failure to protect and secure Plaintiff's and Class members' Private Information in compliance with applicable laws and industry standards would result in that Information being accessed and stolen by unauthorized actors.

125. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered, and continue to suffer, injuries and damages arising from the unauthorized access of their Private Information, including but not limited to theft of their personal information, damages from the lost time and effort to mitigate the impact of the Data Breach, and permanently increased risk of identity theft.

126. Plaintiff and Class members are entitled to damages in an amount to be proven at trial and injunctive relief requiring Defendant to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class members.

COUNT III
BREACH OF IMPLIED CONTRACT
(By Plaintiff on behalf of the Class, or, in the alternative, the North Dakota Subclass)

127. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

128. Plaintiff and the Class provided Defendant with their Private Information.

129. By providing their Private Information, and upon Defendant's acceptance of this information, Plaintiff and the Class, on one hand, and Defendant, on the other hand, entered into implied-in-fact contracts for the provision of data security, separate and apart from any express contract entered into between the parties.

130. The implied contracts between Defendant and Plaintiff and Class members obligated Defendant to take reasonable steps to secure, protect, safeguard, and keep confidential Plaintiff's and Class members' Private Information. The terms of these implied contracts are described in federal laws, state laws, and industry standards, as alleged above. And Defendant expressly adopted and assented to these terms by collecting the Private Information belonging to Plaintiff and the Class.

131. The implied contracts for data security also obligated Defendant to provide Plaintiff and Class members with prompt, timely, and sufficient notice of any and all unauthorized access or theft of their Private Information.

132. Defendant breached these implied contracts by failing to take, develop and implement adequate policies and procedures to safeguard, protect, and secure the Private Information belonging to Plaintiff and Class members; allowing unauthorized persons to access Plaintiff's and Class members' Private Information; and failing to provide prompt, timely, and sufficient notice of the Data Breach to Plaintiff and Class members, as alleged above.

133. As a direct and proximate result of Defendant's breaches of the implied contracts, Plaintiff and the Class have been damaged as described herein, will continue to suffer injuries as detailed above due to the continued risk of exposure of Private Information, and are entitled to damages in an amount to be proven at trial.

COUNT IV
UNJUST ENRICHMENT

(By Plaintiff on behalf of the Class, or, in the alternative, the North Dakota Subclass)

134. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

135. This count is brought in the alternative to Count III.

136. Plaintiff and the Class have a legal and equitable interest in their Private Information that was collected and maintained by Defendant.

137. Defendant was benefitted by the conferral upon it of Plaintiff's and Class members' Private Information and by its ability to retain and use that information. Defendant understood that it was in fact so benefitted.

138. Defendant also understood and appreciated that Plaintiff's and Class members' Private Information was private and confidential and its value depended upon Defendant maintaining the privacy and confidentiality of that information.

139. But for Defendant's willingness and commitment to maintain its privacy and confidentiality, Plaintiff and Class members would not have provided or authorized their Private Information to be provided to Defendant, and Defendant would have been deprived of the competitive and economic advantages it enjoyed by falsely claiming that its data-security safeguards met reasonable standards. These competitive and economic advantages include, without limitation, wrongfully gaining clients and customers, gaining the reputational advantages conferred upon it by Plaintiff and Class members, collecting excessive advertising and sales revenues as described herein, monetary savings resulting from failure to reasonably upgrade and maintain data technology infrastructures, staffing, and expertise raising investment capital as described herein, and realizing excessive profits.

140. As a result of Defendant's wrongful conduct as alleged herein (including, among other things, its deception of Plaintiff, the Class, and the public relating to the nature and scope of the data breach; its failure to employ adequate data security measures; its continued maintenance and use of the Private Information belonging to Plaintiff and Class members without having adequate data security measures; and its other conduct facilitating the theft of that Private Information), Defendant has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and the Class.

141. Defendant's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiff's and Class members' sensitive Private Information, while at the same time failing to maintain that information secure from intrusion.

142. Under the common law doctrine of unjust enrichment, it is inequitable for Defendant to be permitted to retain the benefits it received, and is still receiving, without justification, from Plaintiff and the Class in an unfair and unconscionable manner. Defendant's retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

143. The benefit conferred upon, received, and enjoyed by Defendant was not conferred officiously or gratuitously, and it would be inequitable and unjust for Defendant to retain the benefit.

144. Defendant is therefore liable to Plaintiff and the Class for restitution in the amount of the benefit conferred on Defendant as a result of its wrongful conduct, including specifically the value to Defendant of the PII and medical information that was accessed and exfiltrated in the Data Breach and the profits Defendant receives from the use and sale of that information.

145. Plaintiff and Class members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct.

146. Plaintiff and Class members may not have an adequate remedy at law against Defendant, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT V
VIOLATION OF NORTH DAKOTA
UNLAWFUL SALES OR ADVERTISING PRACTICES ACT

N.D. Cent. Code § 51-15-02, *et seq.*

(By Plaintiff on behalf of the Class, or, in the alternative, the North Dakota Subclass)

147. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

148. Defendant is engaged in, and its acts and omissions affect, trade and commerce. Defendant's relevant acts, practices and omissions complained of in this action were done in the course of Defendant's business of marketing, offering for sale, and selling goods and services throughout North Dakota.

149. The North Dakota Unlawful Sales or Advertising Practices Act ("NDUSAPA") prohibits the use of deceptive or unconscionable acts or practices in the sale or advertisement of any merchandise. N.D. Cent. Code §51-15-02.

150. Defendant's deceptive or unconscionable acts or practices in the conduct of business include, but are not limited to:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class members' Private Information, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents in the industry, which were direct and proximate causes of the Data Breach;

- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' Private Information, including but not limited to duties imposed by the FTC Act, which were direct and proximate causes of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class members' Private Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiff's and Class members' Private Information;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class members' Private Information;
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiff's and Class members' Private Information; and
- h. Failing to promptly and adequately notify Plaintiff and the Class that their Private Information was accessed by unauthorized persons in the Data Breach.

151. Defendant's practices were also contrary to legislatively declared and public policies that seek to protect data and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected in laws, such as HIPAA and the FTC Act.

152. The injuries suffered by Plaintiff and the Class greatly outweigh any potential countervailing benefit to consumers or to competition, and are not injuries that Plaintiff and the Class should or could have reasonably avoided.

153. The damages, ascertainable losses and injuries, including to their money or property, suffered by Plaintiff and the Class as a direct result of Defendant's deceptive acts and practices as set forth herein include, without limitation:

- a. unauthorized charges on their debit and credit card accounts;
- b. theft of their Private Information;

- c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;
- d. loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse effects on their credit scores and adverse credit notations;
- e. costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate and mitigate the actual and future consequences of the Data Breach, including without limitation finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach;
- f. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Private Information being placed in the hands of criminals;
- g. damages to and diminution in value of their personal information entrusted to Defendant, and with the understanding that it would safeguard their data against theft and not allow access and misuse of their data by others; and
- h. the continued risk to their Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as it fails to undertake appropriate and adequate measures to protect data in its possession.

154. Plaintiff and the Class seek all monetary and non-monetary relief allowed by law, including actual or nominal damages; declaratory and injunctive relief, including an injunction barring Defendant from disclosing their Private Information without their consent; reasonable attorneys' fees and costs; and any other relief that is just and proper under NDUSAPA.

COUNT VI
BAILMENT

(By Plaintiff on behalf of the Class, or, in the alternative, the North Dakota Subclass)

155. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

156. Plaintiff's and Class members' Private Information was provided to Defendant.

157. In delivering their Private Information, Plaintiff and Class members intended and understood that their Private Information would be adequately safeguarded and protected.

158. Defendant accepted Plaintiff's and Class members' Private Information.

159. By accepting possession of Plaintiff's and Class members' Private Information, Defendant understood that Plaintiff and the Class expected their Private Information to be adequately safeguarded and protected. Accordingly, a bailment (or deposit) was established for the mutual benefit of the parties.

160. During the bailment (or deposit), Defendant owed a duty to Plaintiff and the Class to exercise reasonable care, diligence, and prudence in protecting their Private Information.

161. Defendant breached its duty of care by failing to take appropriate measures to safeguard and protect Plaintiff's and Class members' Private Information, resulting in the unlawful and unauthorized access to and misuse of Plaintiff's and Class members' Private Information.

162. Defendant further breached its duty to safeguard Plaintiff's and Class members' Private Information by failing to timely notify them that their Private Information had been compromised as a result of the Data Breach.

163. Defendant failed to return, purge, or delete the Private Information belonging to Plaintiff and Class members at the conclusion of the bailment (or deposit) and within the time limits allowed by law.

164. As a direct and proximate result of Defendant's breach of its duty, Plaintiff's and Class members PII that was entrusted to Defendant during the bailment (or deposit) was damaged and its value diminished.

165. As a direct and proximate result of Defendant's breach of its duties, Plaintiff and the Class suffered consequential damages that were reasonably foreseeable to Defendant, including but not limited to the damages set forth herein.

COUNT VII
INTRUSION UPON SECLUSION

(By Plaintiff on behalf of the Class, or, in the alternative, the North Dakota Subclass)

166. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

167. Plaintiff and Class members had a reasonable expectation of privacy in the Private Information that Defendant possessed and/or continues to possess.

168. By failing to keep Plaintiff's and Class members' Private Information safe, and by misusing and/or disclosing their Private Information to unauthorized parties for unauthorized use, Defendant invaded Plaintiff's and Class members' privacy by:

- a. Intruding into their private affairs in a manner that would be highly offensive to a reasonable person; and
- b. Publicizing private facts about Plaintiff and Class members, which is highly offensive to a reasonable person.

169. Defendant knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiff's position would consider Defendant's actions highly offensive.

170. Defendant invaded Plaintiff's and Class members' right to privacy and intruded into Plaintiff's and Class members' private affairs by misusing and/or disclosing their private information without their informed, voluntary, affirmative, and clear consent.

171. As a proximate result of such misuse and disclosures, Plaintiff's and Class members' reasonable expectation of privacy in their Private Information was unduly frustrated and thwarted. Defendant's conduct amounted to a serious invasion of Plaintiff's and Class members' protected privacy interests.

172. In failing to protect Plaintiff's and Class members' Private Information, and in misusing and/or disclosing their Private Information, Defendant has acted with malice and oppression and in conscious disregard of Plaintiff's and the Class members rights to have such information kept confidential and private, in failing to provide adequate notice, and in placing its own economic, corporate, and legal interests above the privacy interests of its thousands of clients and clients' clients. Plaintiff, therefore, seeks an award of damages, including punitive damages, on behalf of Plaintiff and the Class.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually, and on behalf of all members of the Class, respectfully request that the Court enter judgment in her favor and against Defendant, as follows:

- A. That the Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of Federal Rules of Civil Procedure; declare that Plaintiff is a proper class representative; and appoint Plaintiff's Counsel as Class Counsel;
- B. That the Court grant permanent injunctive relief to prohibit Defendant from continuing to engage in the unlawful acts, omissions, and practices described herein;
- C. That the Court award Plaintiff and the Class members compensatory, consequential, and general damages in an amount to be determined at trial;
- D. That the Court award Plaintiff and the Class members statutory damages, and punitive or exemplary damages, to the extent permitted by law;
- E. That the Court award to Plaintiff the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;
- F. That the Court award pre- and post-judgment interest at the maximum legal rate;
- G. That the Court award grant all such equitable relief as it deems proper and just, including, but not limited to, disgorgement and restitution; and
- H. That the Court grant all other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of herself and the putative Class, demand a trial by jury on all issues so triable.

Date: September 20, 2023

Respectfully Submitted,

By: /s/ Timothy Q. Purdon

ROBINS KAPLAN LLP

Timothy Q. Purdon (ND # 05392)
1207 West Divide Avenue, Suite 200
Bismarck, ND 58501
701-255-3000
tpurdon@robinskaplan.com

Jennifer W. Sprengel (*pro hac vice* anticipated)

Nickolas J. Hagman (*pro hac vice* anticipated)

Alex Lee (*pro hac vice* anticipated)

**CAFFERTY CLOBES MERIWETHER
& SPRENGEL LLP**

135 S. LaSalle, Suite 3210
Chicago, Illinois 60603
Telephone: (312) 782-4880
Facsimile: (312) 782-4485
jsprengel@caffertyclobes.com
nhagman@caffertyclobes.com
alee@caffertyclobes.com

Attorneys for Plaintiff and the Proposed Class